

Many POS terminals handle credit card or debit card payments and thus also include a magstripe reader. Some have fingerprint readers (discussed in the next section) that read your fingerprint, which is linked to a payment method such as a checking account or credit card. After swiping your card through the reader or reading your fingerprint, the POS terminal connects to a system that authenticates the purchase. Once the transaction is approved, the terminal prints a receipt for the customer.

A self-service POS terminal allows consumers to perform all checkout-related activities (Figure 5-40). That is, they scan the items, bag the items, and pay for the items themselves. Consumers with small orders find the self-service POS terminals convenient because these terminals often eliminate the hassle of waiting in long lines.



FIGURE 5-40 Many grocery stores offer self-serve checkouts, where the consumers themselves use the POS terminals to scan purchases, scan their store saver card and coupons, and then pay for the goods.

Automated Teller Machines

An **automated teller machine (ATM)** is a self-service banking machine that connects to a host computer through a network (Figure 5-41). Banks place ATMs in convenient locations, including grocery stores, convenience stores, retail outlets, shopping malls, and gas stations, so that customers conveniently can access their bank accounts.

Using an ATM, people withdraw cash, deposit money, transfer funds, or inquire about an account balance. Some ATMs have a touch screen; others have special buttons or keypads for entering input. To access a bank account, you insert a plastic bankcard in the ATM's magstripe reader. The ATM asks you to enter a password,

called a *personal identification number (PIN)*, which verifies that you are the holder of the bankcard. When your transaction is complete, the ATM prints a receipt for your records.



FIGURE 5-41 An ATM is a self-service banking terminal that allows customers to access their bank accounts.

BIOMETRIC INPUT

Biometrics is the technology of authenticating a person's identity by verifying a personal characteristic. Biometric devices grant users access to programs, systems, or rooms by analyzing some biometric identifier. A *biometric identifier* is a physiological (related to physical or chemical activities in the body) or behavioral characteristic. Examples include fingerprints, hand geometry, facial features, voice, signatures, and eye patterns.

A *biometric device* translates a personal characteristic (the input) into a digital code that is compared with a digital code stored in the computer. If the digital code in the computer does not match the personal characteristic's code, the computer denies access to the individual.

The most widely used biometric device today is a fingerprint reader. A **fingerprint reader**, or

scanner, captures curves and indentations of a fingerprint. With the cost of fingerprint readers less than \$100, home and small business users install fingerprint readers to authenticate users before they can access a personal computer. External fingerprint readers usually plug into a USB port. To save on desk space, some newer keyboards and notebook computers have a fingerprint reader built into them, which allows users to log on to programs and Web sites via their fingerprint instead of entering a user name and password (Figure 5-42). Grocery and retail stores now use fingerprint readers as a means of payment, where the customer's fingerprint is linked to a payment method such as a checking account or credit card. For a technical discussion about fingerprint readers, read the High-Tech Talk article on page 268.

A *face recognition system* captures a live face image and compares it with a stored image to determine if the person is a legitimate user. Some buildings use face recognition systems to secure access to rooms. Law enforcement, surveillance systems, and airports use face recognition to protect the public. Some notebook computers use this security technique to safeguard a computer. The computer will not start unless the user is legitimate. These programs are becoming more sophisticated and can recognize people with or without glasses, makeup, or jewelry, and with new hairstyles.

Biometric devices measure the shape and size of a person's hand using a *hand geometry system* (Figure 5-43). Because their cost is more than \$1,000, larger companies use these systems as time and attendance devices or as security devices. Colleges use hand geometry systems to verify students' identities. Day-care centers and hospital nurseries use them to verify parents who pick up their children.

A *voice verification system* compares a person's live speech with their stored voice pattern. Larger organizations sometimes use voice verification systems as time and attendance devices. Many companies also use this technology for access to sensitive files and networks. Some financial services use voice verification systems to secure telephone banking transactions. These systems use speaker-dependent voice recognition software. That is, users train the computer to recognize their inflection patterns.



FIGURE 5-42 Keyboard with built-in fingerprint reader.



FIGURE 5-43 A hand geometry system verifies this student's identity before he is allowed access to the school library.

A *signature verification system* recognizes the shape of your handwritten signature, as well as measures the pressure exerted and the motion used to write the signature. Signature verification systems use a specialized pen and tablet.

High security areas use iris recognition systems. The camera in an *iris recognition system* uses iris recognition technology to read patterns in the iris of the eye (Figure 5-44). These patterns are as unique as a fingerprint. Iris recognition systems are quite expensive and are used by government security organizations, the military, and financial institutions that deal with highly sensitive data. Some organizations use *retinal scanners*, which work similarly but instead scan patterns of blood vessels in the back of the retina.

Sometimes, fingerprint, iris, retina, and other biometric data are stored on a smart card. A



WEB LINK 5-9

Biometric Input

For more information, visit scs.site.com/dc2009/ch5/weblink and then click Biometric Input.



FIGURE 5-44 An iris recognition system.

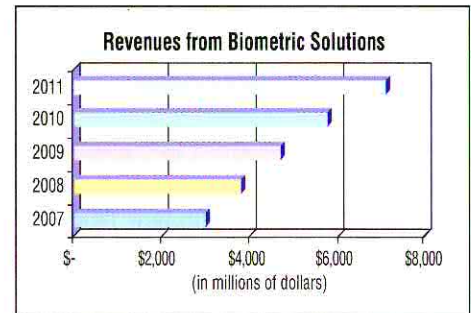
smart card, which is comparable in size to a credit card or ATM card, stores the personal data on a thin microprocessor embedded in the card (Figure 5-45). Smart cards add an extra layer of protection. For example, when a user places a smart card through a smart card reader, the computer compares a fingerprint stored on the card with the one read by the fingerprint reader. Some credit cards are smart cards; that is, the microprocessor contains the card holder's information instead of a magnetic stripe.



FAQ 5-10

How popular is biometric technology?

One study estimates that revenues from biometric solutions have and will continue to grow by about 22 percent annually for the next several years, as shown in the chart below. For more information, visit scs.site.com/dc2009/ch5/faq and then click Biometrics.



Source: International Biometric Group



FIGURE 5-45 A smart card reader reads data stored on a smart card's microprocessor.

High-Tech Talk

BIOMETRICS: PERSONALIZED SECURITY

Biometric authentication is based on the measurement of an individual's unique physiological and behavioral characteristics. The most common measurements, described earlier in this chapter, such as fingerprints, hand geometry, facial features, and eye patterns are physiological biometrics. Some of the more novel measurements, such as body odor, brain wave patterns, DNA, ear shape, sweat pores, and vein patterns also fall into the category of physiological biometrics. Voice scan and signature scan are examples of behavioral biometrics.

Any biometric technology process involves two basic steps — enrollment and matching. To illustrate these steps, this High-Tech Talk uses the most common biometric technology, finger-scan technology.

ENROLLMENT Enrollment is the process in which a user presents the fingerprint data to be stored in a template for future use, as shown in the top of Figure 5-50. This initial template is called the *enrollment template*. Creating the enrollment template involves four basic steps: (1) acquire fingerprint, (2) extract fingerprint feature, (3) create enrollment template, and (4) store enrollment template. The enrollment template usually is created only after the user has submitted several samples of the same fingerprint. Most fingerprint images will have false details, usually caused by cuts, scars, or even dirt, which must be filtered out.

The first step, acquire fingerprint, presents a major challenge to finger-scan technology. The quality of a fingerprint may vary substantially from person to person and even finger to finger. The two main methods of acquiring images are optical and silicon. With optical technology, a camera is used to register the fingerprint image against a plastic or glass platen (scanner). Silicon technology uses a silicon chip as a platen, which usually produces a higher quality fingerprint image than optical devices.

The second step, extract fingerprint feature, involves thinning the ridges of the raw image to a minuscule size and then converting the characteristics to binary format. Fingerprints are comprised of ridges and valleys that have unique patterns, such as arches, loops, and swirls. Irregularities and discontinuities in these ridges and valleys are known as *minutiae*. Minutiae are the distinctive characteristics upon which most finger-scan technology is based. The fingerprint-feature extraction process used is highly sophisticated, patented, and a closely-held vendor secret.

In the third step, the binary format is used to create the enrollment template. The fourth and final step involves storing the template on a storage device, such as a hard disk or smart card for future use when the same person attempts to be authenticated.

MATCHING Matching is the process of comparing a match template to an enrollment template. A *match template* is created when the user attempts to gain access through a fingerprint reader. Most computer and network systems are set up so that the person also must claim an identity, such as a user name, along with the fingerprint. In this case, the match template is compared directly to the enrollment template for that user name. Other systems, such as those used for criminal investigations, will search the entire enrollment template database for a match.

The match template is created in the same fashion as the enrollment template described earlier. Rather than storing the match template on disk, however, it is compared to the user's stored enrollment template, as shown in the bottom of Figure 5-50. The result of the matching process is a score. The score is compared against a threshold.

The threshold is a predefined number that can be adjusted depending on the desired level of security.

The scoring process leads to the decision process. The decision process will produce one of three actions: (1) the threshold has been exceeded, thereby resulting in a match; (2) the threshold has not been met, thereby resulting in a nonmatch; or (3) the data may have been insufficient, resulting in the system requesting a new sample from the user to begin a new comparison.

Finger-scan technology has grown to become the centerpiece of the biometric industry. For more information, visit scs.site.com/dc2009/ch5/tech and then click Biometrics.

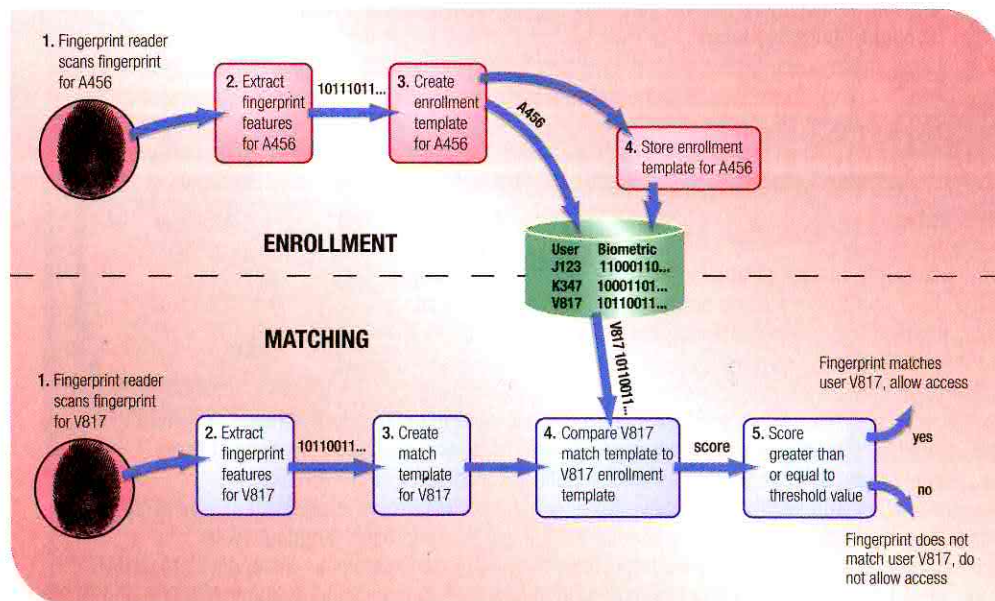


FIGURE 5-50 The two steps in biometric technology.